NT-Cryptography
MAT4930 *7554*

Class-X

Prof. JLF King
1Sep2015

X4:	___	___	55pts
X5:	___	___	75pts
X6:	___	___	25pts
Total:	___ ___	___	155pts

X4: *Show no work. Please write* **DNE** *in a blank if the described object does not exist or if the indicated operation cannot be performed.*

a Modulo 35, the multiplicative-order of 3 is .... [*Hint:* $\varphi(35)$ has very few prime factors.]

b Let $f(x) := x^2 - 9x + 14$, and $N := 28225 \overset{\text{note}}{=\!=} p \cdot 25$, where $p := 1129$ is prime. The *number* of solns $x \in [0 .. N)$ to $\boxed{f(x) \equiv_N 0}$ is $K=$ .... A number $Z \in [0 .. N)$ such that $f(Z) \neq 0$ yet $f(Z) \equiv_N 0$ is ....

[*Hint:* Find solns mod-p and mod-25, then use CRT.]

Essay questions, OYOSOP:

X5: i For functions $f,g{:}\,\mathbb{Z}_+ \to \mathbb{C}$, define carefully their ***Dirichlet convolution*** $f \circledast g$.

ii Give a non-trivial example of Dirichlet convolution. Evaluate your convolution at some (actual) non-trivial value.

iii [Main] Prove that if f and g are each multiplicative fncs (***MF***), then so is $f \circledast g$.

iv Give an example of a **non**-MF f [with $f(1) = 1$] and an MF g, for which $H := f \circledast g$ is *not* an MF. (Evaluate H at a value which *shows* H not a MF.)

X6: Use Pollard-ρ to find a non-trivial factor of $N := 10403$, using seed $s_0 := 4$ and map $f(x) := 2{+}x^2$. Make a nice table, labeled

Time	Tortoise	Hare	$s_{2k} - s_k$	Gcd(??)

—*but* ***replace*** *the "??" with the correct expression.* You found non-trivial factor $E :=$ ....

[*Fact:* Your table has $\leqslant$4 lines.]

End of Class-X